BINARY BCH codes CORRECTING ℓ errors

$n = 2^m - 1$, $k = 2^m - \ell m - 1$

$d = 2\ell + 1$

(Generalization of cyclic Hamming codes and double error correcting BCH)

Construct $\mathbb{Z}_2^m$

Let $\alpha \in \mathbb{Z}_2^m$ is primitive

$P(\alpha) = 0$ $\deg P(x) = m$.

TAKE

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \dots & \alpha^{5(n-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2\ell-1} & \alpha^{2(2\ell-1)} & & \dots & \alpha^{(n-1)(2\ell-1)} \end{bmatrix}$$

EXAMPLE $\quad m=8 \qquad n=2^8-1=255$

$\ell=5 \qquad d=11$

$$K = 255 - 5\cdot 8 = 215$$

FOR ℓ- error correcting BCH codes we have

$$R = \frac{K}{n} = \frac{2^m - \ell\cdot m - 1}{2^m-1} = 1 - \frac{\ell m}{2^m - 1}$$

For small ℓ $R \to 1$

Let $\mathbb{C}$ is ℓ-error correcting BCH

and $v \in \mathbb{C}$ $\Rightarrow$

$$\begin{cases} v(\alpha) = 0 \\ v(\alpha^3) = 0. \\ v(\alpha^5) = 0 \\ \cdots\cdots \\ v(\alpha^{2\ell-1}) = 0 \end{cases}$$

Thus $\mathbb{C}$ contain all polynomials with ℓ different roots $\alpha, \alpha^3, \alpha^5, \dots, \alpha^{2\ell-1}$

$\mathbb{C}$ is cyclic

Decoding of BCH codes

Example $\ell = 3$ $\quad (d = 7)$

$$S = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \end{bmatrix} = H\,e = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \dots & \alpha^{5(n-1)} \end{bmatrix} e$$

Let $e = (0 \dots 0 \underset{i}{1} 0 \dots 0 \underset{j}{1} 0 \dots 0 \underset{s}{1} 0 \dots 0) \Rightarrow$

errors are in bits i, j, s

Then

$$\begin{cases} S_1 = \alpha^{i} + \alpha^{j} + \alpha^{s} \\ S_2 = \alpha^{3i} + \alpha^{3j} + \alpha^{3s} \\ S_3 = \alpha^{5i} + \alpha^{5j} + \alpha^{5s} \end{cases}$$

Denote

$$x=\alpha^{i}\ ,\ y=\alpha^{j}\ ,\ z=\alpha^{s}$$

$$\begin{cases} S_1 = x+y+z \\ S_2 = x^3+y^3+z^3 \\ S_3 = x^5+y^5+z^5 \end{cases}$$

this is the system of three equations with 3 unknowns x, y, z and has a unique solution.

Decoding is complex.

$$S_1, S_2, S_3 \underset{\text{difficult}}{\longrightarrow} x, y, z \underset{\text{easy.}}{\longrightarrow} i, j, s$$

EXTENDED BCH CODES

Let H_{BCH} is a check matrix for $n = 2^m - 1$, $k = 2^m - \ell m - 1$, $d = 2\ell + 1$ ℓ-error correcting code

Consider

$$H = \begin{array}{c} \overbrace{\hphantom{H_{BCH}\quad\;\; 0}}^{n+1} \\ \left[\begin{array}{c|c} H_{BCH} & \begin{matrix}0 \\ \vdots \\ 0\end{matrix} \\ \hline 1\ 1 \cdots\ 1 & 1 \end{array}\right] \end{array} \begin{array}{l} \left.\vphantom{\begin{matrix}0 \\ \vdots \\ 0 \\ 1\end{matrix}}\right\} \ell m + 1 \\ \text{overall parity} \end{array}$$

H is the check matrix for $n = 2^m$, $k = 2^m - \ell m - 1$, $d = 2\ell + 2$ extended BCH code

By extending and shortening BCH codes with any distance and any length can be constructed

<u>Example</u> Construct a code with length $n=24$ and distance $d=6$

1) Take $m=5$ and construct BCH with $n=2^5-1=31$ and

$k=2^5-1-2\cdot 5=21$ $(\ell=2)$

$d_{BCH}=5$

2) Extend the constructed BCH

Then $n=32$, $k=21$, $d=6$

3) Shorten this code by deleting $i=32-24=8$ columns in its check matrix. Then finally we have:

$n=24$, $k=13$, $d=6$

$\therefore$ Codes obtained by extension and shortening of BCH are good for small $\frac{d}{n}$

e.g. $d=5$ $(\ell=2)$

DOUBLE ERROR CORRECTING CYCLIC CODES (BCH codes)

$n = 2^m - 1$, $k = 2^m - 2m - 1$, $d = 5$.

BINARY case: $q = 2$

Consider the field Z_2^m

Construct a code of length $n = 2^m - 1$ with check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \dots & \alpha^{3(n-1)} \end{bmatrix}$$

where α is primitive element in Z_2^m

EXAMPLE : $m=4$.

BIN	EXP
0000	0
0001	1
0010	α
0011	α^4
0100	α^2
0101	α^8
0110	α^5
0111	α^{10}
1000	α^3
1001	α^{14}
1010	α^9
1011	α^7
1100	α^6
1101	α^{13}
1110	α^{11}
1111	α^{12}

$\alpha^3 \alpha^2 \alpha \, 1$

$P(x) = x^4 + x + 1$

$\alpha^4 = \alpha + 1$

$\alpha^5 = \alpha^2 + \alpha$

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$

$\alpha^8 = \alpha^2 + 1$

$\alpha^9 = \alpha^3 + \alpha$

$\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$

$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$

$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$

$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1$

$\alpha^{15} = \alpha^4 + \alpha = 1$

$$\alpha^{15} = 1$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

$$= \begin{array}{c} \begin{array}{ccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \end{array} \\ \left[\begin{array}{ccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \end{array}$$

$\mathbb{C}$ is $(15, 2^7, 5)$ BCH code.

$v \in C \implies Hv = 0$

$$0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{12} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ \vdots \\ v_{15} \end{bmatrix}$$

$v \in C \Rightarrow$

$$\begin{cases} v_1 + \alpha v_2 + \alpha^2 v_3 + \alpha^3 v_4 + \dots + \alpha^{14} v_{15} = 0 \\ v_1 + \alpha^3 v_2 + \alpha^6 v_3 + \alpha^9 v_4 + \dots + \alpha^{42} v_{15} = 0 \end{cases}$$

Thus

$$v(x) = v_1 + x v_2 + x^2 v_3 + x^3 v_4 + \dots + x^{14} v_{15}$$

and $\begin{cases} v(\alpha) = 0 \\ v(\alpha^3) = 0 \end{cases}$

Thus

$$v \in C \Leftrightarrow v(\alpha) = 0 \text{ and } v(\alpha^3) = 0.$$

BCH code consists of all polynomials with roots α and α^3

Let $v \in \mathbb{C}$

consider w

where $w(x) = v(x)\,Q(x)$

for <u>any</u> $Q(x)$

then $w(\alpha) = v(\alpha)\,Q(\alpha) = 0$

$w(\alpha^3) = v(\alpha^3)\,Q(\alpha^3) = 0 \Rightarrow$

$w \in \mathbb{C}$

If $v \in \mathbb{C}$ any w such that

$w(x) = v(x)\,Q(x)$ ~~being~~ belongs

to $\mathbb{C}$

Thus $\mathbb{C}$ is cyclic.

Decoding Double Error Correcting BCH codes with $d=5$

Let $v \to v+e \qquad v \in C$

$S = H(v+e) = Hv + He = He$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(n-1)} \end{bmatrix}$$

1. For single errors

$$e = (0\,0 \dots 0\,\overset{i}{1}\,0 \dots 0)$$ – bit i is distorted

Then $S = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} \alpha^i \\ \alpha^{3i} \end{bmatrix}$

$S_1 = \alpha^i \qquad S_2 = \alpha^{3i}$

thus iff $S_1^3 = S_2 \Rightarrow$

single error occur $(\ell = 1)$

and the error is in the

bit i iff $S_1 = \alpha^i$

For the previous example of

$(15, 2^7, 5)$ BCH code

iff $S = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ \cdot \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \cdots \\ \alpha^6 \end{bmatrix}$ $\quad S_1 = \alpha^7$, $S_2 = \alpha^6$

Since $(\alpha^7)^3 = \alpha^{21} = \alpha^6 \qquad (\alpha^{15} = \alpha^0)$

we have that bit 7 is distorted

For double errors $\ell = 2$

$$e = (0 \ldots 0 \overset{i}{1} 0 \ldots 0 \overset{j}{1} 0 \ldots 0)$$

$$S = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} \alpha^i + \alpha^j \\ \alpha^{3i} + \alpha^{3j} \end{bmatrix}$$

$$S_1^3 \neq S_2 \Rightarrow \ell \neq 1.$$

Denote $\alpha^i = y$ $\alpha^j = z$

we have the following system of two equations with two unknowns y, z:

$$\begin{cases} y + z = S_1 \\ y^3 + z^3 = S_2 \end{cases}$$

Since $y \neq z \Rightarrow S_1 \neq 0$

Then

$$S_2 \cdot S_1^{-1} = y^2 + yz + z^2$$

$$S_1 = y + z$$

$$S_1^2 = y^2 + z^2$$

$$S_2 \cdot S_1^{-1} = S_1^2 + yz$$

Thus we have the system

$$\begin{cases} y + z = S_1 \\ yz = S_2 \cdot S_1^{-1} + S_1^2 \end{cases}$$

If there are two errors this system is solvable for y, z.

$$y = \alpha^i, \quad z = \alpha^j$$

Thus if we know S_1, S_2
we can compute y, z and
then locations of errors i and j.

Decoding procedure is complex
which is the main disadvantage
of BCH codes.

BINARY BCH codes (Revisited)

Let $n = 2^m - 1$ consider $GF(2^m)$

α primitive in $GF(2^m)$

$P(x)$ primitive generating $GF(2^m)$

$\alpha \in GF(2^m)$, $P(\alpha) = 0$, $\deg P(x) = m$

Check matrix for $(2^m - 1, 2^{2^m - \ell m - 1}, 2\ell + 1)$

cyclic BCH code $\mathbb{C}$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha^{(2\ell-1)} & \alpha^{2(2\ell-1)} & \dots & \alpha^{(2\ell-1)(n-1)} \end{bmatrix} \quad r = \ell m$$

$\mathbb{C}$ consists of all polynomials

$$v(x) = v_0 + v_1 x + \dots + v_{n-1} x^{n-1} \qquad (v_i \in \{0, 1\})$$

such that $v(\alpha) = v(\alpha^3) = v(\alpha^5) = \dots = v(\alpha^{2\ell-1}) = 0$.

Note that if $a_1, a_2, \dots, a_s \in GF(2^m)$ then

$$(a_1 + a_2 + \dots + a_s)^2 = a_1^2 + a_2^2 + \dots + a_s^2 \qquad (*)$$

Thus $v(\alpha^2) = v_0 + v_1 \alpha^2 + v_2 \alpha^4 + \dots + v_{n-1} \alpha^{2(n-1)} =$

$$= (v_0 + v_1 \alpha + v_2 \alpha^2 + \dots + v_{n-1} \alpha^{n-1})^2 = 0$$

Since $v_i = v_i^2 \qquad (v_i \in \{0, 1\})$

Similarly, if $v \in C$ where

$\mathbb{C}$ is $(2^m-1, 2^{2^m-\ell m-1}, 2\ell+1)$ BCH code

$$v(\alpha^2) = v(\alpha^4) = \ldots = v(\alpha^{2\ell}) = 0 \qquad (1)$$

thus $v \in C \Leftrightarrow$

$$v(\alpha^i) = 0 \qquad (i = 1, \ldots, 2\ell) \qquad d = 2\ell+1$$

Conditions (1) should not be verified for computing syndrome since they follow automatically for binary BCH from (*)